Notice of Allowability	Application No.	Applicant(s)	
	09/401,596	CHESS, DAVID M	
	Examiner	Art Unit	
	Neveen Abel-Jalil	2165	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *November 24, 2004*.

2. ☒ The allowed claim(s) is/are *2-14,16-28,30-32 and 34-41*.

3. ☒ The drawings filed on *September 22, 1999* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

C. Rones

CHARLES RONES
PRIMARY EXAMINER

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 24-November -2004 has been entered.

2. The amendment filed on 24-November -2004 has been received and entered. Claims 1, 15, 29, and 33 have been cancelled. Claims 38-41 have been newly added. Therefore, claims 2-14, 16-28, 30-32, and 34-41 are pending.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Paul D. Greeley (Attorney of Record) on January 4, 2005, and again on March 31, 2005.

4. The application has been amended as follows:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listings of Claims:

Claim 1 (Canceled)

Claim 2 (Previously Presented) A method as in claim 38, wherein the stored object information is descriptive at least in part of a number and location of macros within the object.

Claim 3 (Previously Presented) A method as in claim 38, wherein the stored object information is descriptive at least in part of a number and location of archived objects within the object.

Claim 4 (Previously Presented) A method as in claim 38, wherein the stored object information is descriptive at least in part of features of the object that serve as inputs to a neural network-based virus detection system, and wherein the step of programmatically examining the object comprises a step of operating the neural network-based virus detection system using the features as inputs.

Claim 5 (Previously Presented) A method as in claim 38, wherein the stored object information is descriptive at least in part of whether at least one macro is present within the object.

Claim 6 (Previously Presented) A method as in claim 38, wherein the stored object information is descriptive at least in part of whether at least one archived object is present within the object.

Claim 7 (Previously Presented) A method as in claim 38, wherein the stored 2ob information is descriptive at least in part of whether the object can possibly be infected with a virus according to predetermined criteria, and wherein the step of programmatically examining is executed only if the stored object information indicates that the object may possibly be infected according to the predetermined criteria as compared to criteria that are currently in effect.

Claim 8 (Previously Presented) A method as in claim 38, wherein if it is indicated that a current state of the object is not described by the stored object information, the step of programmatically examining comprises an initial step of processing the object to ascertain the current state of the object, and storing information in the object-state database that is descriptive of the current state of the object.

Claim 9 (Previously Presented) A method as in claim 38, wherein the stored object information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of whether the at least one contained object is of a type that should be examined for computer viruses, and wherein the step of programmatically examining avoids re-determining and re-scanning the contained at least one object if the stored object information indicates that the at least one contained object is not required to be scanned.

Claim 10 (Previously Presented) A method as in claim 38, wherein the stored object information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of at least one of a location, extent, or encoding-method of the at least one contained object, and wherein the step of programmatically examining is responsive to the stored object information for reducing an amount of processing time required to extract the at least one contained object in order to examine the at least one contained object.

Claim 11 (Previously Presented) A method as in claim 38, wherein the stored object information comprises information descriptive of a location of an entry-point of the object, and wherein the step of programmatically examining uses the stored object information to determine the entry-point of the object, if the object-state database indicates that the object has not changed since the entry-point information was stored.

Claim 12 (Previously Presented) A method as in claim 38, wherein the stored object information comprises information descriptive of a structure of the object, and wherein the step of programmatically examining uses the stored object information to determine the structure of the object, if the object-state database indicates that the object has not changed since the structure information was stored.

Claim 13 (Previously Presented) A method as in claim 38, wherein the stored object information comprises information descriptive of at least one of a number, size, name, extent, or other attribute of macros or other units of active content in the object, and wherein the step of

programmatically examining uses the stored object information to determine at least one of the number, size, name, extent, or other attribute of macros or other units of active content in the object, if the object-state database indicates that the object has not changed since the information was stored.

Claim 14 (Previously Presented) A method as in claim 38, wherein the step of programmatically examining includes a program-emulation step for executing the current object in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results produced by the program-emulation step in the object-state database, and wherein the step of programmatically examining uses the stored results rather than re-executing the program-emulation step, if the object-state database indicates that the object has not changed since the results were stored.

Claim 15 (Canceled)

Claim 16 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information is descriptive at least in part of a number and location of macros within the object.

Claim 17 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information is descriptive at least in part of a number and location of archived objects within the object.

Claim 18 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information is descriptive at least in part of features of the object that serve as inputs to a neural network-based virus detection system, and wherein said neural network-based virus detection system uses the features as inputs.

Claim 19 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information is descriptive at least in part of whether at least one macro is present within the object.

Claim 20 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information is descriptive at least in part of whether at least one archived object is present within the object.

Claim 21 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information is descriptive at least in part of whether the object can possibly be infected with a virus according to predetermined criteria, and wherein said object examination unit programmatically examines said object only if the stored object information indicates that the object may possibly be infected according to the predetermined criteria as compared to criteria that are currently in effect.

Claim 22 (Previously Presented) A virus detection component as in claim 39, wherein if said determination indicates that a current state of the object is not described by the information stored in said database, said object examination unit first processes the object to ascertain the current state of the object, and stores information in said object-state database that is descriptive of the current state of the object.

Claim 23 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of whether the at least one contained object is of a type that should be examined for computer viruses, and wherein said object examination unit inhibits re-determining and re-scanning the contained at least one object if the stored object information indicates that the at least one contained object is not required to be scanned.

Claim 24 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information comprises, for an object that contains in archived or combined form at least one other object, information descriptive of at least one of a location, extent, or encoding-method of the at least one contained object, and wherein said object examination unit is responsive to the stored object information for reducing an amount of processing time required to extract the at least one contained object in order to examine the at least one contained object.

Claim 25 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information comprises information descriptive of a location of an entry-point of the

object, and wherein said object examination unit is responsive to the stored object information to determine the entry-point of the object, if the object-state database indicates that the object has not changed since the entry-point information was stored.

Claim 26 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information comprises information descriptive of a structure of the object, and wherein said object examination unit is responsive to the stored object information for determining the structure of the object, if the object-state database indicates that the object has not changed since the structure information was stored.

Claim 27 (Previously Presented) A virus detection component as in claim 39, wherein the stored object information comprises information descriptive of at least one of a number, size, name, extent, or other attribute of macros or other units of active content in the object, and wherein said object examination unit is responsive to the stored object information for determining at least one of the number, size, name, extent, or other attribute of macros or other units of active content in the object, if the object-state database indicates that the object has not changed since the information was stored.

Claim 28 (Previously Presented) A virus detection component as in claim 39, and further comprising a program-emulation unit for executing the current object in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results produced by the program-emulation unit in said database, and wherein said

object examination unit is responsive to the stored results for using said stored results, and for inhibiting the operation of said program emulation unit, if the object-state database indicates that the object has not changed since the results were stored.

Claim 29. (Canceled)

Claim 30 (Previously Presented) A computer program as in claim 40, wherein said computer readable medium further stores a list comprised of information that is descriptive of at least one of known viruses and of known classes of viruses, said list being used by said object examination code segment when programmatically examining the object for the presence of a computer virus.

Claim 31 (Previously Presented) A computer program as in claim 40, wherein said computer readable medium further stores a neural network-based virus detection code segment, wherein said object-state database further stores information descriptive of features of the object that serve as inputs to said neural network based virus detection code segment, and wherein said neural network-based virus detection code segment uses the features as inputs.

Claim 32 (Previously Presented) A computer program as in claim 40, wherein said computer readable medium further stores a program-emulation code segment for executing objects in a virtual environment, for collecting data resulting from the execution in the virtual environment, and for storing at least some of the results in said database, and wherein said object examination unit code segment is responsive to the stored results for using said stored results, and for

inhibiting the operation of said program emulation unit code segment, if said o sect-state database indicates that the object has not changed since the results were stored.

Claim 33. (Canceled)

Claim 34 (Previously Presented) A computer program as in claim 3341, wherein the stored object information is descriptive at least in part of a number and location of macros within the object.

Claim 35 (Previously Presented) A computer program as in claim 341, wherein the stored oJect information is descriptive at least in part of a number and location of archived objects within the object.

Claim 36 (Previously Presented) A computer program as in claim 41, wherein the computer program implements or has access to a neural network-based virus detection system, wherein the stored object information is descriptive at least in part of features of the object that serve as inputs to the neural network-based virus detection system, and wherein the step of programmatically examining the object comprises a step of operating the neural network-based virus detection system using the features as inputs.

Claim 37 (Previously Presented) A computer program as in claim 41, wherein for an object that the object-state database indicates has a current state that is not described by the stored object

information, the step of programmatically examining comprises an initial step of operating the stored program to process the object to ascertain the current state of the object, and storing information in the object-state database that is descriptive of the current state of the object.

Claim 38 (Currently Amended) A virus detection method for use in a computer system, comprising steps of:

providing an object-state database comprised of stored object information that is descriptive of a state of at least one object that ~~may potentially become infected~~ is subject to infection by a computer virus and that reflects the state on object as it existed at a point in the past;

providing a virus-detection database comprised of virus-detection information used in programmatically examining objects for the presence of various computer viruses;

for a current scan of said object that is indicated as having a current state that is described by the stored object information, determining whether or not said object appears to have changed since said point in the past; and

in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examining said object for a presence of a computer virus while making use of the stored object information during the examination.

Claim 39 (Currently Amended) A virus detection component for use in a computer system, comprising:

an object-state database comprised of stored object information that is descriptive of a state of at least one object that ~~may potentially become infected~~ is subject to infection by a computer virus and that reflects the state of said object as it existed at a point in the past;

a virus-detection database comprised of virus-detection information used in programmatically examining objects for the presence of various computer viruses; and

an object examination unit, which, for a current scan of said object that is indicated as having a current state that is described by the stored object information, determines whether or not said object appears to have changed since said point in the past; and which, in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examines said object for a presence of a computer virus while making use of the stored object information during the examination.

Claim 40 (Currently Amended) A computer program embodied on a computer-readable medium for providing a virus detection program subsystem, comprising:

a code segment that at least maintains an object-state database comprised of stored object information that is descriptive of a state of at least one object that ~~may potentially become infected~~ is subject to infection by a computer virus and that reflects the state of said object as it existed at a point in the past;

a virus detecting code segment that at least maintains a virus-detection database comprised of virus-detection information used in programmatically examining objects for the presence of various computer viruses; and

an examination code segment, which, for a current scan of said object that is indicated as having a current state that is described by the stored object information, determines whether or not said object appears to have changed since said point in the past; and which, in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examines said object for a presence of a computer virus while making use of the stored object information during the examination.

Claim 41 (Currently Amended) A computer program embodied on a computer-readable medium, the computer program being capable of executing a method for use in a computer system that comprises at least one object that ~~may potentially become infected~~ is subject to infection with a computer virus, the method executed by the computer program comprising steps of:

maintaining an object-state database comprised of stored object information that is descriptive of a state of at least one object that ~~may potentially become infected~~ is subject to infection by a computer virus and that reflects the state of said object as it existed at a point in the past;

maintaining a virus-detection database comprised of virus-detection information used in programmatically examining objects for the presence of various computer viruses;

for a current scan of said object that is indicated as having a current state that is described by the stored object information, determining whether or not said object appears to have changed since said point in the past; and

in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examining said object for a presence of a computer virus while making use of the stored object information during the examination.

Reasons for Allowance

5. Claims 2-14, 16-28, 30-32, and 34-41 are allowed over the prior art made of record.

6. The following is a statement of reasons for allowance:

The prior art of record (Chen et al. -U.S. Patent No. 5,960,170, and Dotan -U.S. Patent No. 5,822,517) do not disclose, teach, or suggest the claimed limitations of (in combination with all other features in the claim), in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examining said object for a presence of a computer virus while making use of the stored object information during the examination, as claimed in claim 38.

Claims 2-14 are allowed over the prior art made of record, because it is dependent from the allowed independent claim 38.

The prior art of record (Chen et al. -U.S. Patent No. 5,960,170, and Dotan -U.S. Patent No. 5,822,517) do not disclose, teach, or suggest the claimed limitations of (in combination with

all other features in the claim), in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examines said object for a presence of a computer virus while making use of the stored object information during the examination, as claimed in claim 39.

Claims 16-28 are allowed over the prior art made of record, because it is dependent from the allowed independent claim 39.

The prior art of record (Chen et al. -U.S. Patent No. 5,960,170, and Dotan -U.S. Patent No. 5,822,517) do not disclose, teach, or suggest the claimed limitations of (in combination with all other features in the claim), in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said point in the past, programmatically examines said object for a presence of a computer virus while making use of the stored object information during the examination, as claimed in claim 40.

Claims 30-32 are allowed over the prior art made of record, because it is dependent from the allowed independent claim 40.

The prior art of record (Chen et al. -U.S. Patent No. 5,960,170, and Dotan -U.S. Patent No. 5,822,517) do not disclose, teach, or suggest the claimed limitations of (in combination with all other features in the claim), in the case that said object does not appear to have changed since said point in the past, but said virus-detection database does appear to have changed since said

point in the past, programmatically examining said object for a presence of a computer virus while making use of the stored object information during the examination, as claimed in claim 41.

Claims 34-37 are allowed over the prior art made of record, because it is dependent from the allowed independent claim 41.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Neveen Abel-Jalil whose telephone number is 571-272-4074. The examiner can normally be reached on 8:30AM-5: 30PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on 571-272-4038. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Neveen Abel-Jalil
March 31, 2005

C. Rones
CHARLES RONES
PRIMARY EXAMINER